Filter By Service

- Software Escrow & Verification
- Cyber Security
- Risk Management & Governance
- Corporate
- Business Insights
- Careers

Filter By Date

- 2019
- 2018
- 2017
- 2016
- 2015
- 2014
- 2013
- 2012

Door Control Systems: An Examination of Lines of Attack

Introduction

Over recent years many businesses have, in the interest of security, turned to the use of computerised door control systems. These systems, which usually require the entrant to possess some sort of token or swipe card which is authenticated against a central database, are intended to ensure that nobody can enter a business' premises (or restricted sections of those premises) without the proper authorisation.

While no system is perfect, most attempts thus far to circumvent these systems have revolved around either the social aspects (tailgating and so forth) or the possession of the necessary token.

But it is also possible for attackers to attempt to gain entry by exploiting weaknesses in the software and hardware in the door control systems themselves.

In this blog post, we shall show that there are serious security vulnerabilities in one of the market-leading door control systems, and that these can be exploited not only to gain physical access to secure premises, but also to obtain confidential information about the organisation to whom the premises belong.

The weaknesses found include, but are not limited to, missing passwords in the default configuration, control ports that do not allow authentication, a lack of authentication on the door hardware, the ability to copy the database to a machine under the attacker's control, an ability to perform a denial of service attack using a buffer overflow exploit, and hard-coded keys allowing spoofing of user credentials.

To prevent any malicious exploitation whilst the vendor addresses these issues, we shall not name the door control system in question, and certain technical details have been redacted. We plan to publish a fuller version of this paper, including these details, once the vendor has had an opportunity to fix these problems.

We have attempted a broad overview of the security of these systems rather than researching any one area in depth, and so several further lines of research suggest themselves. These are outlined in the Opportunities for Further Research section.

As a result of this research, we would suggest that organisations should attempt, as much as possible, to isolate their physical security systems from their networks, in order to minimise the possibility of a compromise in one system leading to a breach in the other.

Background

We obtained a door control system supplied by a major UK provider, one with a large market share. This system consists of two components - a software-based management server, running on a Microsoft Windows PC; and a door controller, a bespoke piece of hardware which itself runs several software components in order to connect to the management server.

During this research, we attempted to identify the footprint offered by this system, and to discover any weaknesses in the system, especially those that would allow unauthenticated access.

The Door Controller

The door controller we examined was the most recent model available from the manufacturer in question, and as such should allow for a realistic assessment of the current risks from this type of system.

Each door controller consists of a bespoke piece of hardware (the controller itself), which is powered by a battery. This is connected to up to two doors, each of which has an entry (and if necessary an exit) reader and a lock. There is also an auxiliary input for entering PINs and an output - a status light used to show when the door is open.

Most importantly, however, the controller is connected to the management server. In older models, this is through a serial connection, but in more recent models IP-based connectivity is also an option.

This connection is provided through the addition of a popular serial-to-Ethernet device.

The serial-to-Ethernet device can be managed remotely, via both web and telnet, and in the default configuration neither the web interface nor the telnet access have a password configured.

The door controller offers several services to the network in its default configuration. We will discuss the vulnerabilities found in these below:

Control Port

This control port allows the device to be configured. While the specifications of the protocol used have not been published, several third-party researchers have posted the information on the Internet.

This service neither requires nor supports authentication, and commands can be sent via UDP either directly to the target host or to the broadcast address to poll all devices in the broadcast domain.

Notably, if a password has been set for the web and telnet interfaces, and a Get Configuration request is sent to this port, then the password will be included in the response. This will not be the case if the Advanced Password option has been selected in the control panel, but will be true for basic mode (the default configuration).

Passwords in basic mode are also extremely vulnerable even without this, as they cannot be longer than five characters.

It was also possible to set a new IP address for the door controller. This effectively functions as a denial-of-service attack, since the management server becomes unable to communicate with the door controller. It is also necessary to do this for an attacker to take control of the controller itself - only one connection is allowed by the serial-to-IP converter, and the management server attempts to keep a continuous connection. Breaking this connection between the management server and the door controller is necessary before the door can be controlled by the attacker.

Once the IP address is changed, as there is no authentication to prevent the door control system from being reconfigured, the system can be altered and even new software installed on the system, and an attacker can then gain complete control over the associated doors.

The Management Server

In its default setting, without a firewall enabled, the management server exposes a number of services to the network:

Remote Configuration Service

There is a remote configuration port, but port scanning causes this to crash, so it may not always be seen.

The remote configuration server, once a connection has been made, reads in four bytes, which are used to create a buffer, before reading in the command. Should the buffer be too large, the application crashes - thus it is trivially easy to cause a denial of service, and can even be done accidentally. This does not, however, allow the remote execution of code.

The application also uses standard Windows API calls, with a hardcoded key, to encrypt and decrypt data travelling between client and server, making them easy to intercept and spoof. The messages themselves were in a human-readable XML form.

Database Manager

The database manager provides network access in order to allow backups to be started and stopped remotely. It is possible to access this without providing any credentials, and use it to create a backup copy of the database on a machine under the user's control.

(Proof of concept code for this has been developed, but has been redacted while this vulnerability remains open).

Doing this would not only provide an attacker with access to confidential information (such as employee names and PIN numbers if any), it could also be used in conjunction with the IP address changing described in section 4.1.

After importing the database into their own copy of the control software, an attacker could then change the IP address of the door controller, and connect to it with their own server. This would result in the attacker gaining complete control of the doors, while still allowing authorised users to authenticate as normal, thus removing any suspicion.

Evidence gained from reverse engineering suggests that at one point the database manager allowed restoration from backups - meaning that an attacker could replace the database on the server with their own version - but this is no longer the case in the version that was tested. This may be a vulnerability in earlier versions, however.

It is also possible to prevent legitimate backups from being performed - if an incorrect or inaccessible backup destination is specified, the job remains in the queue and further jobs build up behind it.

Other Software

A separate software module, which we will not name here to avoid identification, handles the communication between software and hardware components. This service maintains a constant connection, logging information at all times.

This service handles adding and deleting card numbers, and on examining the messages sent, while we were unable to completely decode the messages due to time constraints, we noted that the only encryption on the card numbers themselves was for them to be XORd with a constant.

Opportunities for Further Research

As the messages sent between the software and hardware components do not appear to be timestamped, it may be possible to replay messages and send them to a second door controller to add a card. However, for this attack to be attempted, the initial handshake would need to be decoded, and this has not yet been achieved.

It was also noted that the communication between software and hardware components includes a regular polling message, sent at consistent intervals. The same handful of messages were sent repeatedly. These have yet to be decoded, but it is probable that further research would prove these to be predictable and easy to emulate.

Another area that presents opportunities for further research is cracking passwords set with the Advanced Password option, and to gain access to user accounts this way.

Summary of Vulnerabilities Found

Default Configuration

The serial-to-Ethernet device has a web server running with no password set.

Control Port Unauthenticated

The control port does not require a password to reconfigure the device. No option to set one was seen.

Password Retrieval

The password for telnet and web access can be retrieved via the control port when basic password mode is in use.

Management Interfaces Unauthenticated

In the default configuration the management services have no password assigned, allowing unauthorised access to the management server.

Denial of Service

The IP address of the device can be changed, preventing the management console from being able to control the doors or view information.

Device Takeover

There is no authentication preventing reconfiguration of the door control system. If the IP address can be changed, the door control system can be reset and configured using an installation controlled by the attacker. This would allow an attacker to gain complete control of the doors.

No Authentication for Database Manager

The database manager requires no authentication, allowing backups to be made to locations controlled by the attacker.

Hard Coded Encryption Key

The remote configuration server uses a hard-coded encryption key, allowing attackers to spoof messages and decrypt information in transit.

Card Numbers XORd

Rather than encrypt card numbers, the software that communicates between the software and hardware merely XORs them with a constant.

Conclusions

While door control systems may provide some defence against a casual or unskilled attacker, our examination of a leading system shows that even using relatively simple technical attacks, it is possible to gain control of these systems. Certainly they provide little defence against a serious attempt at compromise.

We have identified a number of vulnerabilities in this system, ranging from those which are rectifiable by

users to deeper flaws which will require action by the vendor to resolve. Most notably, the lack of authentication for either the control port or the database manager mean that it is possible for an attacker to gain complete control over the door systems without this being readily apparent to users.

There is a pressing need for further research in this area, as this preliminary report suggests that many physical security systems provide little or no protection against the determined attacker.

Given this, it is essential that physical security systems be isolated from corporate networks and domains. An attacker who gains access, even at a fairly low level, to a network, would be able to gain complete control over the organisation's physical security with a very small amount of effort.

We recommend that all physical security systems - not just door controls, but also closed circuit TV systems and anything else that affects a building's physical security - should enforce an air gap between those systems and any networks. In our view this would be a minimum necessary step for any organisation wishing to protect its physical assets.

Published date: 30 September 2013

Written by: Cyber Security Expert

Call us on:
+44 161 209 5200

Newsroom & Events
Newsroom (Ext. website)
Blogs

About Us
History
Board & Senior Management
Careers
Resources
Office Locations

Latest from @NCCGroupplc

©2019 NCC Group.
All rights reserved.

Investor Relations
Share Price
Results & Presentations
Stock Exchange Announcements

Legal
Terms & Conditions
Privacy Policy
Cookie Policy

NCC Group uses cookies to ensure the best experience on our website. You can use this tool to change your cookie settings.

› Cookie settings

Accept all cookies